DETAILED ACTION

1. In view of the Appeal Brief filed on 3/2/2009, PROSECUTION IS HEREBY REOPENED.

2. The text of those sections of Title 35, U.S. Code not included in this section can be found in the prior office action.

EXAMINER'S AMENDMENT

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Mark Haynes on 6/16/2009. Please see attached Interview Summary.

The application has been amended as follows.

In the claims:

1. (canceled).

2. (previously presented) The method of claim 31, including using said associated session key in response to another request to initiate a communication session from a third station received by the first station during said particular session key initiation interval, and using other session keys from the set of ephemeral session keys after expiry of said particular session key initiation interval.

3. (previously presented) The method of claim 2, including associating a unique set of intermediate data keys with each session key.

4. (amended) The method of claim 31, including:
providing a buffer at the first station;
storing the set of ephemeral session keys in the buffer; and
removing session keys from said buffer upon expiry of respective session key lifetime.

5. (canceled).

6. (previously presented) The method of claim 4, wherein the session key lifetimes have respective lengths longer or equal to a time required for verification of mutual authentication using said first and second sets of exchanges in expected circumstances.

7. (canceled)

8. (canceled).

9. (previously presented) The apparatus of claim 34, including logic to use said associated session key in response to another request to initiate a communication session from a third station received by the first station during

said particular session key initiation interval, and using other session keys from the set of ephemeral session keys after expiry of said particular session key initiation interval.

10. (previously presented) The apparatus of claim 9, including logic to associate a unique set of intermediate data keys with each session key.

11. (amended) The apparatus of claim 34, including
a buffer at the first station;
logic to store the set of ephemeral session keys in the buffer and to remove session keys in said set of ephemeral session keys from said buffer after expiry of the respective session key lifetimes.

12. (canceled).

13. (previously presented) The apparatus of claim 11, wherein the session key lifetimes have respective lengths longer or equal to a time required for verification of mutual authentication using said first and second sets of exchanges.

14-30. (canceled).

31. (amended) A method for mutual authentication in communications between first and second stations, comprising:
generating and storing a set of ephemeral session keys at the first station, ephemeral session keys in the set being associated with respective session key initiation intervals, and being discarded upon expiry of respective session key lifetimes at a time later than expiration of the respective session key initiation intervals;

in response to a request to initiate a communication session received by the first station during a particular session key initiation interval, selecting the associated session key;

sending a message carrying said associated session key to the second station, and receiving a response from the second station including a digital identifier, the digital identifier being information shared between the first station and the second station, or between the first station and a user at the second station, the digital identifier being encrypted using said associated session key to verify receipt of the session key by the second station and to identify the second station or the user of the second station;

generating and storing, in the first station, a set of intermediate data keys, the set of intermediate data keys including intermediate data key (i), for i = 1 to at least n, where n is at least 2, and being discarded at a time later than expiration of the particular session key initiation interval;

executing a first set of exchanges including one or more exchanges with the second station, after verifying in said first station receipt of the session key by the second station by decrypting the digital identifier using the associated session key at the first station and positively matching the decrypted digital identifier against an existing entry in a stored list of authorized users, the first set of exchanges including in the i^{th} exchange

sending a message to the second station carrying intermediate data key (i) from said set of intermediate data keys encrypted using the associated session key for a first exchange in first set of exchanges and using the intermediate data key (i-1) for subsequent exchanges in the first set of exchanges,

receiving a response from the second station including a hashed version of intermediate data key (i) encrypted using intermediate data key (i), decrypting the hashed version of the intermediate data key (i), calculating a hashed version of intermediate data key (i) at the first station, and matching the calculated hashed version and the received hashed version

of intermediate data key (i) to verify receipt by the second station of intermediate data key (i);

executing a second set of exchanges for mutual authentication after verifying in said first station receipt of the intermediate data key (n-1) by the second station, including

sending a first message carrying intermediate data key (n) encrypted using a hashed version of a first shared secret,

receiving a response from the second station carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the first shared secret, and decrypting the hashed version of the intermediate data key (n), calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the second station of the first shared secret;

sending a second message carrying intermediate data key (n) encrypted using a hashed version of a second shared secret; and

if the second station sends a response to the second message, carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the second shared secret, after possession by the first station of the second shared secret is verified at the second station, the verifying being accomplished at the second station by decrypting the intermediate data key (n) from the second message using the hashed version of the second shared secret, calculating a hashed version of the intermediate data key (n), and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the first station of the second shared secret, then

receiving the response from the second station, and decrypting the hashed version of the intermediate data key (n) using the hashed version of the second shared secret, calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and

the decrypted hashed version of intermediate data key (n) at the first station to verify mutual authentication of the first and second stations; and if mutual authentication is verified at the first station, then sending a message indicating successful authentication; wherein the session key lifetimes have respective lengths which are longer than said session key initiation intervals, and less than a multiple M times a time required for verification of mutual authentication using said first and second sets of exchanges in expected circumstances, where M is less than or equal to 10.

32. (previously presented) The method of claim 31, wherein said message indicating successful authentication carries a signal encrypted using intermediate data key (n-1) or using another prearranged one of said intermediate data keys (i).

33. (previously presented) The method of claim 31, including using intermediate data key (n) as a symmetrical key to encrypt data during post-authentication in communications between the first and second stations in the communication session.

34. (amended) A data processing apparatus, comprising:
a processor associated with a first station, a communication interface adapted for connection to a communication medium, and memory storing instructions for execution by the data processor, the instructions including
logic to receive a request via the communication interface for initiation of a communication session between a first station and a second station;
logic to provide for mutual authentication in communications between the first station and a second station, comprising:
generating and storing a set of ephemeral session keys at the first station, ephemeral session keys in the set being associated with respective session key initiation intervals, and being discarded upon expiry of respective session key

lifetimes at a time later than expiration of the respective session key initiation intervals;

in response to a request to initiate a communication session received by the first station during a particular session key initiation interval, selecting the associated session key;

sending a message carrying said associated session key to the second station, and receiving a response from the second station including a digital identifier, the digital identifier being information shared between the first station and the second station, or between the first station and a user at the second station, the digital identifier being encrypted using said associated session key to verify receipt of the session key by the second station and to identify the second station or the user of the second station;

generating and storing, in the first station, a set of intermediate data keys, the set of intermediate data keys including intermediate data key (i), for i = 1 to at least n, where n is at least 2, and being discarded at a time later than expiration of the particular session key initiation interval;

executing a first set of exchanges including one or more exchanges with the second station, after verifying in said first station receipt of the session key by the second station by decrypting the digital identifier using the associated session key at the first station and positively matching the decrypted digital identifier against an existing entry in a stored list of authorized users, the first set of exchanges including in the i^{th} exchange

sending a message to the second station carrying intermediate data key (i) from said set of intermediate data keys encrypted using the associated session key for a first exchange in first set of exchanges and using the intermediate data key (i-1) for subsequent exchanges in the first set of exchanges,

receiving a response from the second station including a hashed version of intermediate data key (i) encrypted using intermediate data key (i), and decrypting the hashed version of the intermediate data key (i), calculating

a hashed version of intermediate data key (i) at the first station, and matching the calculated hashed version and the received hashed version of intermediate data key (i) to verify receipt by the second station of intermediate data key (i);

executing a second set of exchanges for mutual authentication after verifying in said first station receipt of the intermediate data key (n-1) by the second station, including

sending a first message carrying intermediate data key (n) encrypted using a hashed version of a first shared secret,

receiving a response from the second station carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the first shared secret, and decrypting the hashed version of the intermediate data key (n) , calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the second station of the first shared secret;

sending a second message carrying intermediate data key (n) encrypted using a hashed version of a second shared secret; and

if the second station sends a response to the second message, carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the second shared secret, after possession by the first station of the second shared secret is verified at the second station, the verifying being accomplished at the second station by decrypting the intermediate data key (n) from the second message using the hashed version of the second shared secret, calculating a hashed version of the intermediate data key (n), and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the first station of the second shared secret, then

receiving the response from the second station, and decrypting the hashed version of the intermediate data key (n) using the hashed version of the

second shared secret, calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) at the first station to verify mutual authentication of the first and second stations; and if mutual authentication is verified at the first station, then sending a message indicating successful authentication; wherein the session key lifetimes have respective lengths which are longer than said session key initiation intervals, and less than a multiple M times a time required for verification of mutual authentication using said first and second sets of exchanges in expected circumstances, where M is less than or equal to 10.

35. (previously presented) The apparatus of claim 34, wherein said message indicating successful authentication carries a signal encrypted using intermediate data key (n-1) or using another prearranged one of said intermediate data keys (i).

36. (previously presented) The apparatus of claim 34, including using intermediate data key (n) as a symmetrical key to encrypt data during post-authentication communications between the first and second stations in the communication session.

37-39. (canceled).

Response to Arguments

4. Applicant's arguments reflected in the action filed 3/2/2009, and in light of the amendments outlined above and discussed during the interview dated 6/16/2009

(please see the attached Interview Summary) has been found persuasive. Accordingly, all rejection has been withdrawn.

Allowable Subject Matter

5. Amended claims 2-4, 6, 9-11, 13, and 31-36, now re-numbered as claims 1-14 are allowed.

Conclusion

6. Any comments considered necessary by the applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "comments on statement of reasons for allowance."

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571 272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2439

Farid Homayounmehr Examiner
Art Unit 2439